CONFIDENTIAL OUTSIDE COUNSEL ONLY

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC., Plaintiffs, v. PALO ALTO NETWORKS, INC., Defendant.	C.A. No. 22-01538 **JURY TRIAL DEMANDED**

SUPPLEMENTAL DECLARATION OF NIALL BROWNE
IN SUPPORT OF DEFENDANT'S PROPOSED PROTECTIVE ORDER

I, Niall Browne, declare:

1. I hold the position of Senior Vice President, Chief Information Security Officer at Palo Alto Networks, Inc. ("Palo Alto Networks" or "PAN"). I respectfully submit this declaration in support of Palo Alto Network's Proposed Protective Order. This declaration is based on my personal knowledge as well as information provided to me by PAN employees at my request.

2. PAN's source code relates to network security platforms used by over 85,000 customers, including 95% of the fortune 100 as well as many government and military branches, including various United States Federal Government agencies and State Government agencies. The very purpose of PAN's products for

which source code is being requested is to provide customers with network security. Unauthorized access or public disclosure of PAN's source code for its network security products would not only cause harm to PAN by exposing its trade secrets and proprietary code, but also present an increased risk of network breaches for PAN's customers that utilize PAN's products to provide network security. Leaked source code can enable third parties to gain insights into the functionality of, and vulnerabilities in, the source code not just impacting PAN but also its private and public sector customers. Further, any leakage of source code would be a significant industry event that results in the deterioration of trust in the entire network security industry.

3. More specifically, key aspects of the risk of leaked source code include: (a) ***Intellectual Property Theft***: If proprietary source code is leaked, it can be stolen by competitors or malicious actors. This can lead to the unauthorized use or replication of software, resulting in financial losses and damage to the organization's intellectual property; (b) ***Security Vulnerabilities***: Leaked source code can reveal the inner workings of a software application, potentially exposing security vulnerabilities, backdoors, or weak points. Hackers can exploit this information to compromise the software or the systems it runs on; (c) ***Loss of Competitive Advantage***: Organizations invest significant resources in developing and maintaining their software. When source code leaks, competitors may gain

insights into an organization's technology stack, algorithms, and business logic, potentially eroding the organization's competitive advantage; (d) ***Reputation Damage***: A source code leak can erode customer trust and damage an organization's reputation. Users may lose confidence in the security and reliability of the software, leading to loss of customers and business opportunities; (e) ***Compliance and Legal Issues***: Depending on the nature of the leaked code, there may be legal and regulatory consequences. Organizations may be subject to lawsuits, fines, or other penalties for failing to protect sensitive source code; (f) ***Compliance Violations***: Depending on the industry, there may be compliance requirements related to the protection of source code and data. A source code leak could lead to non-compliance with these regulations, resulting in legal and financial repercussions; and (g) ***Increased Attack Surface***: Leaked source code can enable attackers to develop more targeted and sophisticated attacks against the software. It can also make it easier for them to find and exploit vulnerabilities.

4. [redacted]

[redacted] The protocols for in-person review include logging the times the authorized reviewer arrives and leaves, ensuring that the authorized reviewer is the only person granted access to the room where the stand-alone computer is located, conducting the review without any additional electronics (e.g., computer, camera, cellphone), and no printing capability. These restrictions associated with in-person review on a stand-alone non-network computer provide a high degree of protection for PAN's source code.

5. PAN has never before produced its network security source code via remote access in litigation. PAN does not have established protocols to permit a third party to conduct remote review of its source code, and developing these protocols would place a significant burden on PAN employees. This would at a minimum require PAN to ensure that the controls in place at the remote site are commensurate with the extensive controls which were custom designed to protect PAN's source code in PAN's secure data centers. [redacted] Duplicating and testing these

[redacted]

controls in a third-party remote access environment would require extensive time and resources.

6. Based on my own personal knowledge as well as my discussion with IT professionals at PAN, providing remote access would heighten the risk of a security breach as compared to in-person review for at least several reasons. First, during in-person review, the authorized reviewer would need to arrive at the office building and be escorted to the source code review room, which effectively eliminates the possibility of an unauthorized individual getting access to the stand-alone, non-networked computer. In contrast, remote access substantially increases the possibility that an unauthorized individual can be present during the review, even if the parties were to undertake the substantial burden of setting up video monitoring.

7. Second, during in-person review, an authorized reviewer would enter the source code review room with only a notepad, and would be required to leave his or her cellphone and other electronics outside of the source code review room. This substantially reduces the risk that the authorized reviewer will take photographs or videos of the source code. During remote review, the safeguard of having the authorized reviewer leaving his or her electronic equipment outside of the room would not be present. This substantially increases the risk of an individual taking photos, videos, or otherwise duplicating the source code during

remote access.

8. Third, to the extent the authorized reviewer is using their own personal computer to remotely access the source code, that computer could itself be compromised, which could result in the leakage occurring in real-time or at an undetermined time in the future, and would not have features like printing, screen printing, USB transfer and Bluetooth transfer disabled. There is minimal likelihood of this occurring with a stand-alone non-networked computer with ports disabled that would be used for in-person review.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 6th day of October, 2023, in San Mateo County, California.

DocuSigned by:
Niall Browne
A4540C1EBD31472...

NIALL BROWNE